Docket No.: S0193.0011
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Gernot Eckstein et al.

Application No.: 10/735,517 Confirmation No.: 1592

Filed: December 11, 2003 Art Unit: 2131

For: Preventing the unwanted external detection of operations in digital integrated circuits Examiner: A. R. Sheikh

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notice of Panel Decision for Pre-Appeal Brief Review, this Appeal Brief is filed within one month from the December 26, 2007 mailing date of the Decision.

This Appeal Brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1205.2:

XII Evidence Appendix
XIII. Related Proceedings Appendix

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is: Infineon Technologies AG.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Pursuant to the Office Action dated July 23, 2007, claims 1-5 and 8 remain rejected under 35 USC 102(e) as being anticipated by Kash et al. (U.S. Patent No. 6,515,304; hereinafter "Kash"), and claims 6, 7, 9, and 10 are rejected under 35 USC 103(a) as being unpatentable over Kash in view of Klughart et al. (U.S. Patent No. 6,396,137; hereinafter "Klughart"). Thus, claims 1-10 are pending in the application, with all pending claims on appeal.

IV. STATUS OF AMENDMENTS

No claim amendments after final Office Action were presented.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The paragraph numbers below refer to those of the published application and are examples of where the claimed features may be found in the application; the paragraph numbers do not necessarily represent an exhaustive list of all portions of the application providing support for the claimed features.

A. Independent claim 1:

Independent claim 1 is directed to a method of preventing the external detection of operations in a digital integrated circuit *[reference numeral 1; paragraph 0018]* comprising an asynchronous circuit *[reference numeral 2; paragraph 0018]*, comprising the method step of time-

varying a supply voltage *[reference numerals 3, 4, 5]* of said asynchronous circuit to time-shift the execution time of operations within said asynchronous circuit *[paragraphs 0020-0021]*.

B. Independent claim 3:

Independent claim 3 is directed to a digital integrated circuit *[reference numeral 1; paragraph 0018]* comprising an asynchronous circuit *[reference numeral 2; paragraph 0018]*, and means for time-varying a supply voltage *[reference numerals 3, 4, 5]* of said asynchronous circuit to time-shift the execution point of operations within said asynchronous circuit *[paragraphs 0020-0021]*.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-5 and 8 were erroneously rejected under 35 USC 102(e) as being anticipated by Kash et al. (U.S. Patent No. 6,515,304; hereinafter "Kash"), and whether claims 6, 7, 9, and 10 were erroneously rejected under 35 USC 103(a) as being unpatentable over Kash in view of Klughart et al. (U.S. Patent No. 6,396,137; hereinafter "Klughart").

VII. ARGUMENT

A. Independent claim 1, and dependent claims 2 and 9:

The claimed invention is concerned with the prevention of unauthorized external access to the operation of an integrated digital circuit. More specifically, the invention is concerned with counter-measures against so-called sidechannel attacks, which are performed by unauthorized parties for analyzing integrated digital circuits, for example, for analyzing coding algorithms performed by cryptocoprocessors.

Typically, integrated circuits are implemented as synchronous circuits, which operate on the basis of a clock signal. It is a standard approach in the prior art to introduce random wait states into the operation of such synchronous circuits to thus randomly delay timing of operation of such synchronous circuits. In a typical approach, an external clock is internally randomly delayed within the synchronous circuit to thus randomly postpone the occurrence of the internal operations along

with the random delay of the clock to thus make it more difficult for unauthorized persons to analyze the internal operations.

Claim 1 refers to "an asynchronous circuit." The Examiner continues to uphold his technically incorrect interpretation of the Kash circuit as an "asynchronous circuit." The term "asynchronous circuit" has a clear technical meaning to one of ordinary skill in the present technical field, i.e., to an electrical engineer. Appellant submitted along with the September 24, 2007 Response as evidence, a definition of an asynchronous circuit as provided by the Encyclopedia "Wikipedia." An asynchronous circuit is a self-timed circuit which is not governed by any clock signal, or which does not operate according to a clock signal. Therefore, an asynchronous circuit is not a circuit operating in accordance with a clock and which generates due to some delays some operations which are not directly correlated to a time-specific event, such as a clock.

Therefore, one skilled in the present field would clearly consider the circuit of Kash to be a synchronous circuit as the same is driven by clock timing signals. This is also true for the Fig. 6 embodiment of Kash in which the external clock is randomly delayed in order to generate a jittered internal chip clock which forms the basis of the operations of the internal clocked circuit. Thus, the internal circuit is a synchronous circuit governed by a clock, although this clock is randomly delayed relative to an external clock. In other words, the jitter or random delay of the clock does not change the nature of the circuit, namely to be a synchronous circuit. The Kash circuit operates in synchronism with the jittered or randomly delayed internal clock.

Referring now to the claim element of "time-varying a supply voltage," the Examiner refers to the text portions of column 3, line 66, to column 4, line 3. However, these text portions of the reference do not refer to the Fig. 6 embodiment of Kash. Rather, the same refers to a technology used for facilitating the non-destructive reverse engineering of a circuit by monitoring the modulation of a reflected light beam by parts of active elements or devices in the integrated circuit. See column 3, lines 51-53. A time-varying voltage across an interface in the integrated circuit produces a time-varying modulation of reflectivity from the interface that can be measured and used to obtain information on time varying voltages. See column 3, line 66, to column 4, line 3. This

technique serves for analyzing the operation of internal parts of an integrated circuit by a reflected light beam and has nothing to do with the variation of a supply voltage of a circuit. Thus, the Examiner's implicit argument that the time variation can be derived from column 3, line 66, to column 4 line 3, of Kash is based on a technical misunderstanding on the Examiner's part.

The Examiner is also incorrect when stating that the second reference to Klughart discloses an integrated circuit that operates in an asynchronous manner which is equivalent to Appellant's invention. Klughart also does not deal with any asynchronous circuits. Rather, this reference establishes an additional security against reverse engineering performed by third parties (see column 34, lines 42-48). Klughart teaches arranging layers of metal and specific semiconductor materials above switches and regulators in integrated circuits to thus prevent unauthorized access by third parties to the operation of these switches and regulators (see column 34, lines 49-64).

The Examiner's allegations that Klughart discloses an asynchronous circuit are not supported by Klughart. The Examiner refers to column 16, lines 49-53. This section of the description does not deal with any asynchronous circuits at all.

The Examiner further refers to column 37, lines 30-35. This section refers to a switching regulator/power converter which asynchronously modulates its pulse width or frequency in order to compensate for changing the load requirements. However, this is not an asynchronous circuit. Therefore, Klughart does not deal with any asynchronous circuit. Moreover, Klughart does not teach or suggest varying the supply voltage of any asynchronous circuit.

Appellant respectfully submits that independent claim 1 and dependent claims 2 and 9 are patentable over the applied references.

B. Independent claim 3, and dependent claims 4-8 and 10:

The claimed invention is concerned with the prevention of unauthorized external access to the operation of an integrated digital circuit. More specifically, the invention is concerned with counter-measures against so-called sidechannel attacks, which are performed by unauthorized

parties for analyzing integrated digital circuits, for example, for analyzing coding algorithms performed by cryptocoprocessors.

Typically, integrated circuits are implemented as synchronous circuits, which operate on the basis of a clock signal. It is a standard approach in the prior art to introduce random wait states into the operation of such synchronous circuits to thus randomly delay timing of operation of such synchronous circuits. In a typical approach, an external clock is internally randomly delayed within the synchronous circuit to thus randomly postpone the occurrence of the internal operations along with the random delay of the clock to thus make it more difficult for unauthorized persons to analyze the internal operations.

Claim 3 refers to "an asynchronous circuit." The Examiner continues to uphold his technically incorrect interpretation of the Kash circuit as an "asynchronous circuit." The term "asynchronous circuit" has a clear technical meaning to one of ordinary skill in the present technical field, i.e., to an electrical engineer. Appellant submitted along with the September 24, 2007 Response as evidence, a definition of an asynchronous circuit as provided by the Encyclopedia "Wikipedia." An asynchronous circuit is a self-timed circuit which is not governed by any clock signal, or which does not operate according to a clock signal. Therefore, an asynchronous circuit is not a circuit operating in accordance with a clock and which generates due to some delays some operations which are not directly correlated to a time-specific event, such as a clock.

Therefore, one skilled in the present field would clearly consider the circuit of Kash to be a synchronous circuit as the same is driven by clock timing signals. This is also true for the Fig. 6 embodiment of Kash in which the external clock is randomly delayed in order to generate a jittered internal chip clock which forms the basis of the operations of the internal clocked circuit. Thus, the internal circuit is a synchronous circuit governed by a clock, although this clock is randomly delayed relative to an external clock. In other words, the jitter or random delay of the clock does not change the nature of the circuit, namely to be a synchronous circuit. The Kash circuit operates in synchronism with the jittered or randomly delayed internal clock.

Referring now to the claimed "means for time-varying a supply voltage," the Examiner refers to the text portions of column 3, line 66, to column 4, line 3. However, these text portions of the reference do not refer to the Fig. 6 embodiment of Kash. Rather, the same refers to a technology used for facilitating the non-destructive reverse engineering of a circuit by monitoring the modulation of a reflected light beam by parts of active elements or devices in the integrated circuit. See column 3, lines 51-53. A time varying voltage across an interface in the integrated circuit produces a time-varying modulation of reflectivity from the interface that can be measured and used to obtain information on time varying voltages. See column 3, line 66, to column 4, line 3. This technique serves for analyzing the operation of internal parts of an integrated circuit by a reflected light beam and has nothing to do with the variation of a supply voltage of a circuit. Thus, the Examiner's implicit argument that the time variation can be derived from column 3, line 66, to column 4 line 3, of Kash is based on a technical misunderstanding on the Examiner's part.

The Examiner is also incorrect when stating that the second reference to Klughart discloses an integrated circuit that operates in an asynchronous manner which is equivalent to Appellant's invention. Klughart also does not deal with any asynchronous circuits. Rather, this reference establishes an additional security against reverse engineering performed by third parties (see column 34, lines 42-48). Klughart teaches arranging layers of metal and specific semiconductor materials above switches and regulators in integrated circuits to thus prevent unauthorized access by third parties to the operation of these switches and regulators (see column 34, lines 49-64).

The Examiner's allegations that Klughart discloses an asynchronous circuit are not supported by Klughart. The Examiner refers to column 16, lines 49-53. This section of the description does not deal with any asynchronous circuits at all.

The Examiner further refers to column 37, lines 30-35. This section refers to a switching regulator/power converter which asynchronously modulates its pulse width or frequency in order to compensate for changing the load requirements. However, this is not an asynchronous circuit. Therefore, Klughart does not deal with any asynchronous circuit. Moreover, Klughart does not teach or suggest varying the supply voltage of any asynchronous circuit.

Appellant respectfully submits that independent claim 3 and dependent claims 4-8 and 10 are patentable over the applied references.

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto in the Claims Appendix.

X. EVIDENCE

As indicated in the Evidence Appendix, no evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

X. RELATED PROCEEDINGS

As indicated in the Related Proceedings Appendix, no related proceedings are referenced in II. above.

Please charge any fee, except for the Issue Fee, that may be necessary for the continued pendency of this application to our Deposit Account No. 50-2215.

Dated: January 16, 2008

Respectfully submitted,

By Laura C. Brutman

Laura C. Brutman
Registration No.: 38,395
DICKSTEIN SHAPIRO LLP
1177 Avenue of the Americas
New York, New York 10036-2714
(212) 277-6500
Attorney for Appellant

CLAIMS APPENDIX

Claims 1-10 are on Appeal

1. A method of preventing the external detection of operations in a digital integrated circuit comprising an asynchronous circuit,

comprising the method step of time-varying a supply voltage of said asynchronous circuit to time-shift the execution time of operations within said asynchronous circuit.

2. The method according to claim 1, wherein the time variation of said supply voltage takes place in a random way.

3. A digital integrated circuit comprising:

an asynchronous circuit, and

means for time-varying a supply voltage of said asynchronous circuit to time-shift the execution point of operations within said asynchronous circuit.

4. The digital integrated circuit according to claim 3, wherein said means for time-varying said supply voltage comprises a random number generator.

5. The digital integrated circuit according to claim 4, wherein said means for time-varying said supply voltage further comprises a noise voltage source driving said random-number generator.

6. The digital integrated circuit according to claim 4, wherein said means for time-varying said supply voltage further comprises a digital-analog converter transforming the digital values produced by said random-number generator into an analog voltage.

7. The digital integrated circuit according to claim 3, wherein said means for time-varying said supply voltage further comprises a voltage regulator.

8. The digital integrated circuit according to claim 3, wherein said asynchronous circuit is formed for executing a coding algorithm.

9. The method according to claim 1, wherein the asynchronous circuit is a type which performs processing without correlation to a clock.

10. The digital integrated circuit according to claim 3, wherein the asynchronous circuit is a type which performs processing without correlation to a clock.

EVIDENCE APPENDIX

All evidence is in the record.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings for this matter.